# CDI Information Security Policy

**To:** CDI Employees

**No.:** ISO-02

**From:** Information Security Office (ISO)

**Issued:** July 1, 2004

**Subject:** Password Policy

**Expires:** When Superseded

## Policy

California Department of Insurance (CDI) passwords must be kept confidential and not be shared among employees. This password policy applies to all CDI systems. Any password that has been compromised, is suspected of having been compromised, or has been revealed to anyone else with the exception of the employee's immediate supervisor must be changed immediately.

## Purpose

To protect CDI's confidential or sensitive data from being accessed by an unauthorized user.

## Procedure

The following standards should be observed when selecting passwords.

**Passwords should:**

- Be comprised of a combination of alphabetic and numeric characters. A number must not be placed at the beginning or end of the password.
- Not contain dates or names of weekdays or months (9/11/2002, Monday, December).
- Not be the same as hobbies, names of family members, or pets.
- Not contain any words, names, or technical terms that can be easily guessed or cracked.

**Passwords must:**

- Be at least eight (8) characters long, or the maximum number of characters that the system or device will accept if less than 8 characters.

- If the system will accept more than 8 characters, a password of at least 8 characters is required.

- Be changed in accordance with password change parameters for each system but at a minimum of every 90 days.

- Not be used again for at least ten (10) changes.

- Not represent any numerical progression (e.g. 246810 [adding two to each number], 392781 [multiplying the number by three], etc.)

- Not be the same as or contain the employee's phone number, Social Security Number (SSN), birth date, address, license plate number, driver's license number, name, nickname, user ID, cubicle number, office name, district name or abbreviations of any of the above.

## Password Protection

The following practices should be observed when using passwords:

- Do not write your password down in plain sight.

- Do not include your password in scripts or macros.

- If anyone asks for a password other than the Information Technology Division (ITD) help desk or the employee's supervisor or manager, the employee should refuse and notify their supervisor or manager immediately.

## Management Access to Passwords

Occasionally, supervisors or managers must have access to passworded CDI equipment during an employee's absence from work or the work site (e.g. unexpected absence or illness, emergency, etc.) to access business related files.

## Compromised or Rejected Passwords

Passwords must be changed immediately if revealed to anyone else or if they are suspected or known to have been compromised. The user ID will be blocked after the password has been incorrectly entered three (3) times. To deter passwords from being guessed or cracked with a common password-cracking program, CDI's network security limits the number of password access attempts.

If an employee enters a correct password but is blocked from using the system, it could indicate that someone has attempted to access the system with the employee's user ID and failed. Any suspected unauthorized use of a user ID or password must be immediately reported by the employee to their supervisor or manager. ITD will monitor failed log on attempts on a monthly basis.

## Password Resume or Reset

If a password is forgotten, the employee must contact the ITD help desk. Before the password or user ID is resumed or reset, the person doing the resume or reset must verify that the person making the request is the owner of the user ID (e.g. telephone the employee's supervisor or manager to verify the employee is in the office and needs their password reset).

## New Employee Passwords

New employees' user IDs and passwords are to adhere to the same standards listed above. The local ITD Administrators assign and set the user ID and password for a new employee. New IDs and passwords should not be set more than 72 hours before the employee's start date. Once the new employee logs on with the assigned password, they are required to immediately set a new password in order to continue logging on to the computer.

## CDI Menu, Fraud Integrated Data Base (FIDB) and all other Passwords

The CDI menu and FIDB passwords are assigned by the ITD help desk, so the ITD help desk must be called to establish a CDI menu logon and password. The assigned temporary password will also prompt the new user to immediately reset the password in order to continue logging on to the CDI Menu or FIDB. These passwords will follow the same guidelines as network passwords.

## Screen Locking Passwords

An active terminal or personal computer (PC) with access to CDI confidential or sensitive information should never be left unattended without logging off or activating a password-protected screensaver. If the user is leaving the visible proximity of the machine, the user must either log off the machine or activate a password-protected screensaver prior to leaving the terminal or PC.

## Inquiries

Please contact the ISO at 916-492-3256 or 916-492-3353 if you have any questions regarding this policy.

________________________________________

Archie Alimagno, Information Security Officer